We claim:

1. A data control system comprising:

a computer platform having hardware; said hardware capable of authenticating an operating system to be loaded on said hardware and preventing said operating system from being loaded onto said hardware when said operating system is not authenticated;

said hardware having memory in which application programs and object files can be stored;

said operating system capable of creating a firewall around data in memory pertaining to application programs and object files to control access to said application programs and object files;

an input interface connected to said platform to allow input data to be received by said platform; said operating system capable of decrypting said input data and of authenticating said input data;

said firewalls around said data in memory being capable of allowing said application programs to access said data in memory when approval of access is obtained from said application program and from said data in memory; and

an output interface connected to said platform to allow said platform to transmit output data out of said platform; said output data being encrypted when transmitted.

2. A data control system as claimed in claim 1, wherein said hardware authenticates said operating system by verifying a digital signature associated with said operating system.

3. A data control system as claimed in claim 1, wherein said operating system decrypts said input data with a private decryption key unique to said platform.

4. A data control system as claimed in claim 1, wherein said operating system authenticates said input data by verifying a digital signature associated with said input data with a public signature key and input data that is not authenticated by said operating system is classified as insecure data.

5. A data control system as claimed in claim 3, further comprising a sending station capable of encrypting data with a public encryption key; said public encryption key being directly related to said private decryption key of said computer platform.

6. A data control system as claimed in claim 4, further comprising a sending station capable of creating a digital signature with a secret signature key; said secret signature key being distinctively associated with said sending station.

7. A data control system as claimed in claim 1, wherein said data in memory gives approval for access through an object handler associated with each of said object files when said data in memory pertains to said object files.

8. A data control system as claimed in claim 1, wherein said output data is encrypted with an encryption key unique to said platform.

9. A data control system as claimed in claim 8, wherein said output data is decrypted with an decryption key associated with said public encryption key.

10. A data control system as claimed in claim 4, wherein said output interface encrypts said output data when said output data includes at least a portion of data that has been authenticated by said operating system.

11. A data control system as claimed in claim 1, wherein said operating system is capable of authenticating said input data by using a hash function.

12. A data control system comprising:

a sending station,

a plurality of receiving platforms, each of said receiving platforms having firmware and an operating system, said firmware authenticating said operating system,

said sending station including: (a) a plurality of application programs, (b) a plurality of object files, (c) a plurality of handler programs, each associated with a separate one of said object files, and (d) a plurality of secret key encoded signatures, each distinctive to a subset of said application programs and said object files,

each of said receiving platforms being adapted to receive said application programs, object files, handlers and signatures,

each of said receiving platforms having: (a) a public signature identification key to authenticate said signatures and (b) firewalls associated with said application programs and object files to control access to each of said application programs and object files,

the one of said handler programs associated with each of said object files permitting access to the associated object files by an appropriate one or more of said application programs.

each of said handler programs being programmable to permit multi-parameter control over access to the associated one of said object files.

13. The data control system of claim 12 wherein: said object files and said application programs at said sending station are encrypted with a public key unique to the receiving platform being addressed and wherein said encrypted object files and application programs are decrypted with a private key, at the receiving platform.

14. The data control system of claim 12 wherein said signature identification is provided through a signature creation algorithm and a secret key at said sending station and through a signature verification algorithm and a public key at each receiving platform.

15. The data control system of claim 13 wherein said signature identification is provided through a signature creation algorithm and a secret key at said sending station and through a signature verification algorithm and a public key at each receiving platform.

16. The system of claim 12 wherein:

said sending station has a plurality of secret key encoded signatures, each signature being distinctive to a separate set of application programs and data texts,

each receiving platform having a plurality of public signature identification keys to correspond to the plurality of secret keys at said sending station.

17. A method for providing a data control system, comprising the steps of:

authenticating an operating system to be loaded on a computer platform; said authenticating step to be performed every time an operating system is loaded on said computer platform;

verifying credentials of data transmitted to said computer platform before loading said data into memory of said computer platform;

creating firewalls around data loaded into memory of said computer platform;

decrypting data transmitted to said computer platform with a private decryption key unique to said computer platform; and encrypting data transferred out of said computer platform with a public encryption key unique to said computer platform and associated with said public decryption key.

18. A method as claimed in claim 17 wherein said authenticating step is performed by verifying a digital signature associated with said operating system.

19. A method as claimed in claim 17 further comprising the step of obtaining permission before allowing an application program to access data loaded into memory.

20. A method as claimed in claim 19 wherein said obtaining step is performed through object handlers.

ABSTRACT

A computer platform is described that provides control features to allow for the protection of intellectual property rights and prevent malfunctioning of the platform. The platform uses 1) a secure operating system including a secure memory management system, 2) public key encryption, 3) data authentication through digital signatures and 4) application/data approval through a flexible access policy through the use of object handlers and an application program approval process. Through these four control features, the platform provides the ability to control access to data and minimize the effects of computer malfunctions.